

September 13, 2010

U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201
Attention: HITECH Privacy and Security Rule Modifications

Re: HITECH Proposal to Modify HIPAA Privacy, Security and Enforcement Rules
RIN 0991-AB57, 75 *Federal Register* 40868, July 14, 2010

Dear Sir or Madam:

The American Bankers Association (ABA)¹ is responding to the above proposal of the Department of Health and Human Services (HSS) to modify the existing Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).² The proposal implements recent statutory amendments under the Health Information Technology for Economic and Clinical Health Act (HITECH Act)³ including the requirement of the HITECH Act that business associates of covered entities comply with the privacy and security requirements of HIPAA. Many of ABA's member banks are business associates of HIPAA covered entities.

Background

The HITECH Act, enacted on February 17, 2009, is designed to promote the widespread adoption and standardization of health information technology. Subtitle D of the Act supports this goal by strengthening the privacy and security protections for health information established by HIPAA, including extending the applicability of the privacy and security standards requirements to the business associates of covered entities.

¹ The American Bankers Association represents banks of all sizes and charters and is the voice for the nation's \$13 trillion banking industry and its 2 million employees.

² Pub. L. 104-191.

³ The HITECH Act was enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5.

Prior to enactment of the HITECH Act, covered entities were required to obtain “business associate agreements” (BAAs) with companies that provided services to them that involved the use or disclosure of “protected health information” (PHI). However, such “business associates” were not directly subject to the requirements of HIPAA. Rather, any misuse or improper disclosure of PHI was dealt with by means of contractual remedies.

Now, however, the HITECH Act makes business associates for the first time directly subject to the provisions of the HIPAA privacy and security standards and subjects them to civil and criminal liability for failure to meet those standards. In addition, the HITECH Act requires that the additional privacy and security requirements be incorporated into existing business associate agreements.

The proposal generally implements these provisions. However, it would revise the definition of “business associate” to include “subcontractors” – persons who, acting on behalf of business associates, create, receive, maintain or transmit PHI on behalf of the business associate. As a result, subcontractors would be directly liable under HIPAA for violations of the privacy or security standards. Neither covered entities nor business associates would be required to have BAAs with subcontractors. Rather, business associates would be required to obtain satisfactory assurances through a written contract or other arrangement from subcontractors that they will comply with the privacy and security standards as set forth in Section 164.504(e)(1)(i) of HHS’ regulations establishing the required elements of a BAA.

Under the proposal, HHS will provide the necessary language to modify BAAs. In addition, the proposal provides a maximum transition period for contract modifications that is one year and 240 days after the publication of a final rule.

Discussion

As noted above, many of ABA’s members provide financial services that involve PHI and, as a result, are business associates under HIPAA. However, our members are separately subject to regulations establishing privacy and security requirements for customers’ personal information under the Gramm-Leach-Bliley Act (GLBA). These regulations require banks to have contracts with third-party vendors (i.e., subcontractors in HHS’ terminology) ensuring that vendors comply with the privacy and security requirements of GLBA.

Under the proposal, business associates would be required to have a “written contract or other arrangement” with subcontractors that includes the elements established for business associate agreements. We understand from our members that many of their contracts with third-party vendors pursuant to GLBA may, in fact, already incorporate those elements. In such instances,

our members would like to avoid the disruption that would necessarily be involved in obtaining a new “BAA” with their subcontractors. Accordingly, we urge HHS to maintain in its final rule, the current language as stated above, rather than requiring business associates to have a separate BAA with subcontractors to comply with the HITECH Act.

If you have any questions concerning ABA’s position, please contact the undersigned.

Sincerely,

A handwritten signature in black ink, reading "Cristeena G. Naser". The signature is written in a cursive style with a large initial "C".

Cristeena G. Naser